ADD
Internet-Draft
Updates: 8484 (if approved)
Intended status: Standards Track
Expires: January 7, 2021

M. Boucadair
Orange
N. Cook
Open-Xchange
T. Reddy
McAfee
D. Wing
Citrix

July 6, 2020

Supporting Redirection for DNS Queries over HTTPS (DoH)
draft-btw-add-rfc8484-clarification-02

Abstract

This document clarifies whether DNS-over-HTTPS (DoH) redirection is allowed, describes potential issues with redirection in DoH, and proposes how DoH redirection might be performed.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document clarifies the intent of DNS-over-HTTPS (DoH) [RFC8484] whether redirection is allowed (Section 4), potential issues with redirection in DoH (Section 5) and subsequently makes some proposals for how service-level (Section 6) and resource-level (Section 7) redirection might be performed.

This document adheres to Section 4.3 of [I-D.ietf-httpbis-bcp56bis] which discusses the need for protocols using HTTP to specify redirect handling to avoid interoperability problems.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

"A/AAAA" is used to refer to "A and/or AAAA records".

3. Discussion

[RFC8484] indicates that the support of HTTP [RFC7540] redirection is one of DoH design goals (Section 1):

> "The described approach is more than a tunnel over HTTP. It establishes default media formatting types for requests and responses but uses normal HTTP content negotiation mechanisms for selecting alternatives that endpoints may prefer in anticipation of serving new use cases. In addition to this media type negotiation, it aligns itself with HTTP features such as caching, redirection, proxying, authentication, and compression.
>
> The integration with HTTP provides a transport suitable for both existing DNS clients and native web applications seeking access to the DNS."

Nevertheless, Section 3 of [RFC8484] indicates the following:

> "This specification does not extend DNS resolution privileges to URIs that are not recognized by the DoH client as configured URIs."

This looks like an internal inconsistency of [RFC8484] that is worth the clarification: is redirection allowed or not?

Also, Section 3 of [RFC8484] indicates that:

> "A DoH client MUST NOT use a different URI simply because it was discovered outside of the client's configuration (such as through HTTP/2 server push) or because a server offers an unsolicited response that appears to be a valid answer to a DNS query."

Nevertheless, [RFC8484] does not:

- specify under which conditions a discovered different URI can be used.

- describe how a different URI can be discovered using HTTP/2 server push. The only available example in the mailing list archives clarifies that server push is an example of unsolicited responses.

  The text was updated late in the publication process to address this comment: https://mailarchive.ietf.org/arch/msg/doh/f_V-tBgB-KRsLZhttx9tGt75cps/. The example provided in the thread (server push) is related to the second part of the above excerpt.

- clarify that unsolicited messages from a configured DoH server should be excluded.

A clarification is proposed in Section 4. This clarification focuses on a "different URI" that might be discovered while communicating with an HTTP server.

Additionally, assuming that redirection is allowed, this specification recommends how it is achieved. This is required because redirection to a domain-based URI requires DNS resolution of that domain name, which creates a potential bootstrapping problem (e.g., If DoH server is the only configured DNS server, redirecting the client to a new server by presenting a name will fail).

4. RFC8484 Update

OLD:

> A DoH client MUST NOT use a different URI simply because it was discovered outside of the client's configuration (such as through HTTP/2 server push) or because a server offers an unsolicited response that appears to be a valid answer to a DNS query.

NEW

> A DoH client MUST NOT use a different URI that was discovered outside of the client's configuration when communicating with HTTP servers except via HTTP redirection from a configured URI (Section 6.4 of [RFC7231]).
>
> Also, a DoH client MUST ignore an unsolicited response (such as through HTTP/2 server push) that appears to be a valid answer to a DNS query unless that response comes from a configured URI (as described in Section 5.3 of [RFC8484]).

5. Issues with Redirection in DoH

There are several potential issues with redirection in DoH, which are summarized below.

The first issue to be considered is whether a new document considering redirection is needed at all. Redirection in HTTP is done on a per-resource basis; if the only functionality required is to redirect all requests to an entirely different server under the same administrative control, then the alternative service mechanism described in [RFC7838] might be sufficient. However, there are restrictions on the use of alternative services; specifically the certificate presented by the alternative service must be valid for

the origin. This restriction means that alternative services cannot be used for use-cases such as redirecting the client to a locally administered DoH server (e.g., resolver or forwarder) which does not have a certificate valid for the origin. Additionally, alternative services suffer from the bootstrapping issue described below.

The second issue with using HTTP redirection is bootstrapping; any client that is relying solely upon a DoH server for resolution must be able to resolve the domain in the redirect response. Even if a DoH client has a plaintext DNS resolver configured, using that resolver is considered as a minimal privacy leakage [RFC8310]. One possible solution is for the DoH client to use the same server that returned the redirect response to perform the resolution, however that may then lead to a further redirect response. Another solution is for the DoH server to include additional information in the response, similar to the "glue" records as defined in [RFC7719].

The final issue is that HTTP redirection is done on a per-resource basis; this presents several problems for DoH:

1. Every GET request with a new query name will require redirection, which is suboptimal. Indeed, a redirect will only affect a unique request, and the DoH client will thus need to contact the origin server for every new request and get redirected, requiring two roundtrips. Also, permanent redirects [RFC7538] for all these queries would bloat the client's HTTP cache.

2. Using POST requests would solve the issue. Nevertheless POST responses are not widely cached as per Section 4.2.3 of [RFC7231], and mandating the use of POST requests for DoH in order to enable redirection hardly seems reasonable.

The above issues would seem to indicate that despite the intention of [RFC8484] to align itself with HTTP redirection, some additional work is required in order for any other mechanism than alternative services (e.g., [RFC7838]) to be deployed with confidence.

The rest of this document considers the issue of redirection at two levels:

1. Service-level Redirect: Similar to alternative services, this would allow a DoH server to redirect a DoH client to an alternative service for all future queries, rather than on a per-resource basis.

2. Resource-Level Redirect: Solving the bootstrapping problem for regular HTTP redirects. Note that this doesn't solve the caching issues described above, and does raise the question of whether

regular HTTP redirection is desirable or worthwhile (i.e., are there any valid use-cases for resource-level redirection in DoH?).

6. Service-Level Redirect

We considered two possibilities for service-level redirect:

1. Extending [RFC7838] by relaxing the host authentication checks.

2. Using a well-known URI to return information about alternative services.

Extending alternative services was considered, but rejected (see Appendix A for the reasons) in favour of the well-known URI approach.

6.1. Well-Known URI

We propose the use of the well-known URI mechanism [RFC8615], with the name "resinfo" to retrieve resolver information, which could include specifying alternative services, through the use of a JSON object in the response payload. A well-known URI would thus look like "https://doh.example.com/.well-known/resinfo".

The example in Figure 1 shows what a JSON object might look like that specified one or more alternative services. The structure of the response is inspired by Section 4.4.2 of [RFC7975].

Note that the response includes "glue" RR information to allow the alternative service to be accessed without further DNS queries, and includes an authenticated domain name to be used for authenticating the alternative service.

```
{
  "associated-resolvers": {
    "adn": [
      {
        "name": "cpe123.example.net",
        "uri-template": [
          "https://cpe123.example.net/dns-query{?dns}"
        ],
        "a": [
          "192.0.2.1",
          "192.0.2.2"
        ],
        "aaaa": [
          "2001:db8::1",
          "2001:db8::2"
        ],
        "ttl": 3600
      }
    ]
  }
}
```

Figure 1: Response Example with Glue RR Information

7. Resource-Level Redirect

Notwithstanding the issues with resource-level redirects described in Section 5, this section describes a proposal for returning the "glue" RRs required to avoid the bootstrapping issue described in that section (but not the roundtrip or caching issues).

Servers supporting DoH redirect MUST support returning the redirect response body mechanism described hereafter.

> Note: "MUST" is used here because resolving the redirect name using Do53 will fail in some configurations, e.g., https://wiki.mozilla.org/Trusted_Recursive_Resolver (network.trr.mode=3).

Concretely, the DoH server returns in the response body a DNS response with an 'application/dns-message' media type as specified in Section 6 of [RFC8484], containing any A and AAAA records for the domain name in the redirect URI, including any CNAMEs.

For example, if the redirect URI contains the domain name "redirect.example.com", and "redirect.example.com" is a CNAME

pointing to "real.example.com", then an example response body would contain:

- A CNAME record for "redirect.example.com"
- Any A records for "real.example.com"
- Any AAAA records for "real.example.com"

This approach is simple; no client or server support of server push is required, and it is also more efficient in terms of the amount of data transmitted.

8. Security Considerations

DoH-related security considerations are discussed in Section 9 of [RFC8484].

Section 9 of [RFC7838] describes security considerations related to the use of alternate services. Relaxing the host authentication requirements would certainly warrant additional security considerations.

9. IANA Considerations

9.1. resinfo Well-Known URI Suffix

This document requests IANA to assign the following well-known URI from the registry available at https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml.

URI suffix: resinfo

Change controller: IETF

Specification document(s): This document

Status: permanent

10. Acknowledgements

Many thanks to Christian Jacquenet, Philippe Fouquart, and Ben Schwartz for the comments.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7538] Reschke, J., "The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)", RFC 7538, DOI 10.17487/RFC7538, April 2015, <https://www.rfc-editor.org/info/rfc7538>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[RFC7838] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", RFC 7838, DOI 10.17487/RFC7838, April 2016, <https://www.rfc-editor.org/info/rfc7838>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

11.2. Informative References

[I-D.ietf-httpbis-bcp56bis]
Nottingham, M., "Building Protocols with HTTP", draft-ietf-httpbis-bcp56bis-09 (work in progress), November 2019.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <https://www.rfc-editor.org/info/rfc7719>.

[RFC7975] Niven-Jenkins, B., Ed. and R. van Brandenburg, Ed., "Request Routing Redirection Interface for Content Delivery Network (CDN) Interconnection", RFC 7975, DOI 10.17487/RFC7975, October 2016, <https://www.rfc-editor.org/info/rfc7975>.

Appendix A. Extending Alternative Services

Section 9.2 of [RFC7838] discusses the possibilities for attackers to hijack the communication to an origin. This is the justification for the requirement in Section 2.1 of [RFC7838] that "Clients MUST have reasonable assurances that the alternative service is under control of and valid for the whole origin.".

However, when a DoH server presents an alternative DoH service to a DoH client, both the origin and alternative service, as well as the DNS queries and responses, must be, by definition, resistant to MITM attacks. Thus it could be argued that in these circumstances, relaxing the host authentication requirements is justified. The relaxation could be limited, e.g., still requiring some relationship between the origin and the alternative, or unlimited, allowing no such relationship to exist.

However the bootstrapping issues described in Section 5 still apply, and there is no mechanism for the DoH server to specify an authenticated domain name to use to authenticate the alternative service, making this proposal unsuitable for deployment.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Neil Cook
Open-Xchange
UK

Email: neil.cook@noware.co.uk

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: TirumaleswarReddy_Konda@McAfee.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com